# SHORT PROJECT

PHASE THREE

HAFIZ NAVEED UDDIN , KAIRIZ CYBER TECHNOLOGIES,

**Phase 3: Security Hardening Report**

**Objective:** Implemented measures to enhance network and endpoint security through segmentation, patch management, access controls, and awareness training.

**Tools Used:** Firewall configurations, VLANs, patch management tools, multi-factor authentication (MFA), endpoint security solutions, host-based firewalls, intrusion detection/prevention systems (HIDS/HIPS).

**Activities Performed:**

1. **Network Segmentation and Traffic Control**
   o Implemented network segmentation to limit attack spread.
   o Created VLANs and configured firewall rules for traffic control.
2. **Patch Management and Maintenance**
   o Ensured all devices and software are regularly updated with the latest patches and security updates.
   o Established a patch management process for ongoing maintenance.
3. **User Permissions and Access Controls**
   o Reviewed and updated user permissions and access controls.
   o Implemented the principle of least privilege for enhanced security.
4. **Authentication and Endpoint Security**
   o Enforced strong authentication mechanisms, including multi-factor authentication (MFA).
   o Installed and configured endpoint security solutions such as antivirus and anti-malware software.
5. **Host-based Firewalls and Intrusion Detection/Prevention Systems (HIDS/HIPS)**
   o Enabled and configured host-based firewalls and intrusion detection/prevention systems.
6. **Security Policies and Procedures**
   o Developed and implemented comprehensive security policies and procedures to guide security practices.
7. **Employee Security Awareness**
   o Conducted security awareness training sessions for employees to educate them on security best practices and potential threats.
8. **Backup and Disaster Recovery**
   o Implemented and tested a robust backup and disaster recovery plan to ensure data availability and recovery during incidents.

**Conclusion:** The completion of Phase 3 has significantly strengthened the security posture of the network and endpoints by implementing robust security measures and enhancing security awareness among employees.